CLAIM AMENDMENTS

1-40 (canceled)

41. (new) A method of protecting software to be run on a wireless device operable for communication with a server over a wireless network, the protected software being stored on the wireless device in encrypted form and requiring a decryption key for successful execution, the server storing a decryption key for decrypting the protected software, and the method including the steps of:

creating at the wireless device an identifier which characterizes the device;

transmitting the identifier from the wireless device to the server;

verifying at the server that use of the protected software by the wireless device is authorized;

in response to the verification, executing at the server a predetermined function to form a derived identifier, the predetermined function operating on at least two variables including the identifier received from the wireless device and the decryption key stored by the server;

transmitting the derived identifier from the server to the wireless device;

executing at the wireless device a second predetermined function to recover a decryption key, the second predetermined function operating on at least two variables including the derived identifier received from the server and the identifier created by the wireless device; and

decrypting at the wireless device the encrypted software using the recovered decryption key to enable execution of the protected software, wherein successful decryption of the protected software is achieved only in the event that the derived identifier has been formed by the predetermined function operating on the identifier of the wireless device on which the protected software is to be run.

42. (new) A method according to claim 41, wherein the server stores a plurality of decryption keys, each decryption key corresponding to respective protected software, the identifier is created to include information characterizing the protected software, and the derived identifier is formed by the predetermined function

operating on the identifier and the decryption key corresponding to the protected software identified by the identifier.

43. (new) A method according to claim 41, wherein the identifier is derived from information which identifies hardware and/or software present at the wireless device.

44. (new) A method according to claim 41, wherein verifying that use of the protected software by the wireless device is authorized comprises effecting a financial transaction or credit check before allowing execution of the predetermined function.

45. (new) A software protection arrangement for protecting software to be run on a wireless device operable for communication over a wireless network, the protected software being provided in encrypted form and requiring a decryption key for successful execution, and the arrangement including:

identifying means operable to create an identifier which characterizes the device on which the protected software is to be run;

an authorization server operable to receive an identifier created by the identifying means and to execute a predetermined function to form a derived identifier, wherein execution of the predetermined function is conditional upon verification of a condition required for authorization of the use of the software, and the predetermined function operates on at least two variables including the received identifier and the decryption key; and

enabling means operable to: receive the derived identifier from the authorization means; execute a second predetermined function to recover a decryption key, the second predetermined function operating on at least two variables including the derived identifier and the identifier; and decrypt the encrypted software using the recovered decryption key to enable execution of the protected software, wherein successful decryption of the protected software is achieved only in the event that the derived identifier has been formed by the predetermined function operating on the identifier of the device on which the protected software is to be run.

46. (new) An arrangement according to claim 45, wherein the identifier further includes information characterizing the protected software, and the authorization means is operable to select a decryption key corresponding to the identified software.

47. (new) An arrangement according to claim 45, wherein the identifier is derived from information which identifies hardware and/or software present at the device.

48. (new) An arrangement according to claim 45, wherein the authorization means is operable to effect a financial transaction or credit check before allowing execution of the predetermined function.

49. (new) An arrangement according to claim 45, wherein the identifying means is operable to create an identifier as aforesaid on each occasion the protected software is to run on the device.

50. (new) An arrangement according to claim 45, in which the identifying means transmits the identifier to the authorization means, over the wireless network.

51. (new) An arrangement according to claim 51, wherein the authorization means is operable to transmit the derived identifier to the enabling means by means of the wireless network.

52. (new) An arrangement according to claim 45, wherein the enabling means and/or the identifying means are provided by software elements associated with the protected software.

53. (new) A wireless device operable for communication with an authorization server over a wireless network, the wireless device storing protected software in encrypted form and including:

identifying means operable to create an identifier which characterizes the wireless device and to transmit the identifier to the authorization server; and

enabling means operable to receive from the authorization server a derived identifier formed by a predetermined function operating on at least two variables including the identifier received from the

wireless device and the decryption key necessary to decrypt the protected software, and the enabling means being further operable to decrypt the encrypted software using the recovered decryption key to enable execution of the protected software, wherein successful decryption of the protected software is achieved only in the event that the derived identifier has been formed by the predetermined function operating on the identifier of the wireless device.

54. (new) A wireless device according to claim 53, wherein the identifier further includes information characterizing the protected software, and the derived identifier is formed by the predetermined function operating on the identifier and the decryption key necessary to decrypt the protected software identified by the identifier.

55. (new) A wireless device according claim 53, wherein the identifier is derived from information which identifies hardware and/or software present at the device.

56. (new) A wireless device according to claim 53, wherein the identifying means is operable to create an identifier as aforesaid on each occasion the protected software is to be run on the device.

57. (new) A wireless device according to claim 56, wherein the enabling means and/or the identifying means are provided by software elements associated with the protected software.

58. (new) A wireless device according to claim 53, wherein the enabling means is operable to execute a second predetermined function to recover the decryption key, the second predetermined function operating on at least two variables including the derived identifier and the identifier created by the identifying means.

59. (new) A server operable for communication with a wireless device over a wireless network, the server storing a decryption key for decrypting protected software stored on the wireless device, wherein the server is operable to:

receive from the wireless device an identifier characterizing the wireless device;

verify that use of the protected software by the wireless device is authorized;

in response to the verification, execute a predetermined function to form a derived identifier, the predetermined function operating on at least two variables including the identifier received from the wireless device and the decryption key stored by the server; and

transmit the derived identifier to the wireless device.

60. (new) A server according to claim 59, wherein the server stores a plurality of decryption keys, each decryption key corresponding to respective protected software, and the identifier includes information characterizing the protected software, the server being operable to form the derived identifier by executing the predetermined function on the identifier and the decryption key corresponding to the protected software identified by the identifier.

61. (new) A server according to claim 59, wherein the server is operable to effect a financial transaction or credit check to verify that use of the protected software by the wireless device is authorized.

62. (new) A storage medium containing computer software which, when installed on one or more devices, is operable to provide a software protection arrangement according to claim 45.

63. (new) A storage medium containing computer software which, when installed on a wireless device, is operable to provide a wireless device according to claim 53.

64. (new) A storage medium containing computer software which, when installed on a server, is operable to provide a server according to claim 59.